UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS

PHILIP SIEFKE, individually and on behalf of all others similarly situated, Plaintiff, v. **TOYOTA MOTOR NORTH AMERICA, INC., PROGRESSIVE CASUALTY INSURANCE COMPANY, CONNECTED ANALYTIC SERVICES,** Defendants.	Case No. 4:25-cv-00406 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Philip Siefke, individually and on behalf of all others similarly situated, brings this action against Defendants Toyota Motor North America, Inc. ("Toyota"), Progressive Casualty Insurance Company ("Progressive"), and Connected Analytic Services ("CAS") (collectively, "Defendants"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts in the public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiff seeks to hold Defendants responsible for the injuries they inflicted on Plaintiff and tens of thousands of similarly situated persons ("Class Members") due to unauthorized collection and dissemination of private information collected from Toyota vehicles owned or leased by the Plaintiff and Class Members. For several years, without Plaintiff's or Class Members' consent, Defendants Toyota and CAS have been collecting from Class Members' vehicles and selling to third parties, including Defendant Progressive, vast amounts of location and vehicle data (including: location, speed, direction, braking and swerving/cornering events, and image and voice data), and other personal identifiable information ("PII" or "Driving Data").

2. Through this action, Plaintiff seeks to remedy these injuries on behalf of himself and all similarly situated individuals whose Driving Data was collected and disseminated by Defendants.

3. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, reimbursement of out-of-pocket costs, and injunctive relief—including a prohibition on unauthorized collection and dissemination of Driving Data by Defendants.

PARTIES

4. Plaintiff Philip Siefke is a resident of Eagle Lake, Florida. He is the owner of a vehicle manufactured by Defendant Toyota, equipped with technology that can track Plaintiff's Driving Data obtained from the vehicle.

5. Defendant Toyota is an American multinational automotive manufacturing company with its headquarters and principal place of business located at 6565 Headquarters Drive, Plano, TX 75024.

6. Defendant Progressive is a company that provides insurance services and products to customers throughout the United States. Progressive's headquarters and principal place of business is located at 300 North Commons Boulevard, Mayfield Village, OH 44143.

7. Defendant CAS is a company that provides data analytics services in the automotive industry. CAS's headquarters and principal place of business is located at 7600 Windrose Avenue, Suite G-240, Plano, TX 75024.

JURISDICTION AND VENUE

8. This Court has original subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

Minimal diversity is established because Plaintiff (and many members of the class) are citizens of states different than that of any of the Defendants.

9. This Court has personal jurisdiction over each of the Defendants because each of them regularly conducts substantial business in this District.

10. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2) and 1391(b)(2), because substantial part of the events giving rise to the claims emanated from activities within this District and Defendants Toyota and CAS are headquartered in this District.

FACTUAL ALLEGATIONS

Modern Cars Collect Voluminous Data About Their Users

11. Mozilla Foundation is an American nonprofit dedicated to privacy protection.[1] In 2023, Mozilla Foundation conducted a research project on data collection practices of car manufacturers. Its researchers were shocked by their findings. In the language of the Mozilla Foundation, "modern cars are a privacy nightmare", and car manufactures have "shifted their focus from selling cars to selling data."[2]

12. As Mozilla Foundation notes, "[t]here's probably no other product that can collect as much information about what you do, where you go, what you say, and even how you move your body […] than your car. And that's an opportunity that ever-industrious car-makers aren't

[1] *Who we are*, Mozilla Foundation, https://foundation.mozilla.org/en/ (last accessed Mar. 22, 2025).
[2] Jen Caltrider, Misha Rykov, Zoe MacDonald (Sept 6, 2023), "What Data Does My Car Collect About Me and Where Does It Go?", Mozilla Foundation, https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ (last accessed Mar. 22, 2025).

letting go to waste. […] From your philosophical beliefs to recordings of your voice, your car can collect a whole lotta information about you."[3]

13. Beyond non-personal data, such as fuel efficiency, tire pressure and engine performance, today's car manufacturers collect sensitive PII, such as GPS locations and frequently used routes, as well as information regarding one's driving style, acceleration and braking patterns, phone contacts, music preferences and call logs.[4]

14. This data collection effort has attracted regulatory attention. For instance, on January 13, 2025, the Texas Attorney General's Office announced a lawsuit against the insurance company Allstate, and its subsidiary, Arity, for allegedly gathering, using, and selling the geolocation and movement data of Texan drivers.[5]

15. Insurance companies, like Defendant Progressive, collect several types of driver behaviors in real-time, including speeding, hard baking, rapid acceleration, and driving at night or at rush hour.[6]

16. Similarly, on February 28, 2024, Senator Edward J. Markey of Massachusetts, a member of the Senate Commerce, Science and Transportation Committee, urged the Federal Trade Commission to investigate the data privacy practices of auto manufacturers. In his letter to FTC

[3] *Id*.
[4] *What Kind of Data Is My Vehicle Collecting?*, AutoPi.io (Updated June 25, 2024), https://www.autopi.io/blog/the-meaning-of-vehicle-data/ (last accessed Mar. 25, 2025).
[5] Kirk J. Nahra, Ali. A. Jessani, Blythe Riggan, *Texas AG Brings First Ever Lawsuit Under a State Comprehensive Privacy Law*, Wilmer Hale (Jan. 21, 2025), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250121-texas-ag-brings-first-ever-lawsuit-under-a-state-comprehensive-privacy-lawas AG Brings First Ever Lawsuit Under a State Comprehensive Privacy Law (last accessed Mar. 26, 2025).
[6] *Texas AG's Lawsuit Against Allstate: What Drivers Need to Know About Data Privacy*, Hoover Rogers (Jan. 30, 2025), https://www.hooverrogers.com/posts/texas-ags-lawsuit-against-allstate-what-drivers-need-to-know-about-data-privacy (last accessed Mar. 26, 2025) (hereinafter, "Texas AG's Lawsuit Against Allstate")

Chair Khan, Senator Markey explained that "automakers are collecting large amounts of data on drivers, passengers and even people outside the vehicle, with little to no oversight."[7]

17. A *New York Times* report explains that for some time now, insurance companies have offered incentives to people who install dongles in their cars or download smartphone apps that monitor their driving. However, drivers have been historically reluctant to participate in these programs. Faced with this user reluctance, vehicle manufacturers, who can collect such data directly from the vehicles, have offered such data for sale directly to the insurance industry.[8]

18. According to the *New York Times*, "[i]n recent years, automakers, including GM, Honda, Kia and Hyundai, have started offering optional features in their connected-car apps that rate people's driving. Some drivers may not realize that, if they turn on these features, the car companies then give information about how they drive to data brokers like LexisNexis."

19. Insurance companies (like Defendant Progressive), data brokers (like Defendant CAS), and automakers (like Defendant Toyota) profit from selling Driving Data to third parties, including: other insurance providers, marketing agencies, law enforcement, and auto finance companies.[9] Insurance companies use Driving Data to assess risk and determine insurance premiums.[10]

20. As this case shows, such Driving Data is collected, used, and offered for sale by Defendants without Class Members' consent, without users consenting or even being informed of

---

[7] "Senator Markey Urges FTC to Investigate Invasive Data Privacy Practices of Automakers" (February 28, 2024) https://www.markey.senate.gov/news/press-releases/senator-markey-urges-ftc-to-investigate-invasive-data-privacy-practices-of-automakers (last accessed April 7, 2024).

[8] Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies*, New York Times (March 11, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html#:~:text=Kia%2C%20Subaru%20and%20Mitsubishi%20also,from%20over%2010%20million%20vehicles.%E2%80%9D (April 7, 2024).

[9] Texas AG's Lawsuit Against Allstate, *supra*.
Hoover Rogers (Jan. 30, 2025), https://www.hooverrogers.com/posts/texas-ags-lawsuit-against-allstate-what-drivers-need-to-know-about-data-privacy (last accessed Mar. 26, 2025)

[10] Texas AG's Lawsuit Against Allstate, *supra*.

this practice, regardless of whether any particular car functions are turned on, and in violation of statutory and common law principles.

Defendants' Policies About Sharing Driving Data

21. Defendants Toyota, Progressive, and CAS all claim in their respective policies about sharing Driving Data (collectively, "Data Sharing Policies") that they do not share Driving Data of Plaintiff and Class Members without their consent.

22. As described herein, however, Defendants' claims in their Data Sharing Policies are false.

A. Toyota's Data Sharing Policies

23. Toyota specifies the types of "Driving Data" collected through its vehicles, as follows:

> **Driving Data**
> We collect your driving behavior data ("Driving Data") ***which includes the acceleration and speed at which your vehicle is driven, travel direction, use of the steering and braking functionality in your vehicle, and vehicle operation data*** (e.g., sensor readings). Driving Data is used to deliver Connected Services to you, and for quality confirmation, data analysis, research, and product development.[11]

24. In its online "Data Sharing" privacy statement, Toyota insists that it will not share customers' Driving Data without their express prior consent:[12]

> **Driving Data**
> We share Driving Data with our affiliates and business partners so we can work together to provide Connected Services to you and for product improvement. ***If you provide express prior consent, we may also share your Driving Data with our affiliates and non-affiliated insurance companies to provide you with usage-based insurance information and offers***. We will also share Driving Data with compatible third-party services and device[s] [that] you authorize. Unless we obtain your consent, we will not provide your Driving Data to other parties for their own purposes or use your Driving Data for our marketing purposes.
> …
> **Aggregated Data Sharing**

[11] *Data Sharing*, Toyota (Mar. 5, 2025), https://www.toyota.com/privacyvts/ (last accessed Mar. 26, 2025)
[12] *Id*.

> We may sometimes share non-identifying or aggregated data with business partners for education and research related to environmental and energy issues, advanced technologies, and usage analysis.[13]

B. Progressive's "Snapshot" Program and Data Sharing Policies

25. Defendant Progressive has a data sharing program called "Snapshot," whereby Progressive "measure[s] a variety of factors related to your driving, including things such as the time of day you drive, sudden changes in speed (hard brakes and rapid accelerations), the amount you drive, and, for customers using the mobile app in some states, how you're using your mobile phone while driving."[14]

26. Progressive acknowledges that "riskier driving based on these factors indicate a greater likelihood of being in an accident and may result in a higher rate at renewal — depending on the state you live in and when you signed up for Snapshot."[15]

27. Through Defendant Progressive's Snapshot data sharing program, Defendant Toyota shares with Progressive Driving Data collected from Class Members' Toyota vehicles. Through this program, Progressive claims that a driver's consent is first required before the data sharing can happen.

28. Progressive promotes Toyota's involvement in the Snapshot data sharing scheme as follows:

> ***Toyota owners who consent to share driving data from vehicles equipped with Toyota data communication modules will have the opportunity to share their information with Progressive for a potential discount on their auto insurance***. This benefit extends to any Toyota customer who purchases a 2018 or newer Toyota Camry, RAV4 or other vehicle model equipped with the latest connected vehicle technology.
>
> Eligible Toyota customers have the ability to enroll in connected services at the point of purchase, through the Toyota Owners website and soon through a new

[13] *Id*.
[14] Snapshot FAQ, *supra*.
[15] *Id*.

> Toyota mobile application. Once enrolled, data is collected that the owner can later consent to share with Progressive for a potential discount on their auto insurance.
> …
> At this time, the following Toyota models can share data for Usage Based Insurance: most trim levels of the 2018 Camry, 2018 Sienna, and 2019 C-HR, and all trim levels of the 2018 Mirai, 2019 Avalon, 2019 Camry, 2019 Corolla Hatchback, 2020 Corolla Sedan, and 2019 RAV4 models.[16]

29. Thus, Defendants Toyota and Progressive acknowledge that those Toyota customers who have purchased certain 2018 or newer Toyota models may have their Driving Data tracked by Toyota and shared with Progressive.

30. While Progressive represents that the consent of an owner of a Toyota vehicle is required before having Driving Data shared with Progressive, this representation is untrue, as shown by events described herein.

C. CAS's Data Sharing Policies

31. CAS is a "consumer reporting agency and data aggregator" that "process[es] data from vehicles equipped with data communication modules."[17] On its website, CAS lists Defendant Toyota as one of its "partners."[18]

32. CAS claims that it is "committed to developing new and exciting ways to leverage data in order to cultivate greater customer satisfaction, refine the insurance pricing process, and help create safer driving conditions."

---

[16] *Toyota Insurance Management Solutions teams up with Progressive Insurance to offer insurance discounts for qualifying customers*, Progressive, https://progressive.mediaroom.com/news-releases/?item=122465 (last accessed Apr. 8, 2025)
[17] *Leveraging Data to Empower Drivers*, Connected Analytic Services, https://connectedanalyticservices.com/ (last accessed Mar. 31, 2025).
[18] *Id*.

33. CAS provides Driver Data shared by its partners, like Defendant Toyota, to insurance carriers, like Defendant Progressive, as provided on CAS's website:

> **Data at Quote**
> With owner consent, we provide insurance carriers with the driving behavior data from connected vehicles at time of quote. No waiting, no delay.
>
> **Data at Purchase**
> Insurance carriers can provide customers with an opportunity to consent to share connected vehicle data on an ongoing basis, no aftermarket devices or mobile applications required.

34. CAS claims to protect driver privacy and data, boasting that "[e]nsuring the utmost privacy and security of our customers is not just a priority; it's our unwavering commitment."[19] As events described here demonstrate, that statement is untrue.

Without Plaintiff's and Class Members' Consent, Toyota Shared Plaintiff's and Class Members' Driving Data with CAS, Who Then Shared the Driving Data with Progressive

35. On or about March 20, 2021, Plaintiff Philip Siefke purchased a 2021 Toyota RAV4 XLE equipped with a "telemetry" tracking device that can track and collect Plaintiff's Driving Data ("Tracking Technology").

36. "Telemetry is a system that allows [one] to collect, measure and monitor data or indicators remotely, **usually through electronic devices and sensors.** Therefore, it is a technology used to capture information from various sources, such as machines, equipment and systems. They will then be transmitted to a central location where they will be analyzed."[20]

37. Examples of Driving Data collected from Toyota vehicles *via* Tracking Technology include: location, fuel levels, odometer, speed, tire pressure, window status, and seatbelt status.[21]

---

[19] *Id.*
[20] *All about telemetry: what it is, how it works and what the benefits are for fleet management*, GolFleet (Feb. 23, 2024), https://golfleet.com.br/en/o-que-e-telemetria/ (last accessed Apr. 8, 2025)
[21] *See Telemetry*, Toyota, https://toyotadatasolutions.com/products#telemetry (last accessed Apr. 7, 2025)

38. On or about January 21, 2025, Plaintiff Siefke attempted to sign up for an insurance policy with Defendant Progressive through Progressive's website.

39. As Plaintiff proceeded with the online process to sign up for an insurance policy, he opted out of Progressive's Snapshot data sharing program.

40. After opting out of the Snapshot program in the online sign up process, however, a background pop-up window appeared, notifying Plaintiff that Progressive was already in possession of his Driving Data up to January 20, 2025.

41. To find out how Progressive obtained Driving Data on Plaintiff, despite him never having participated in the Snapshot program, Plaintiff called Progressive and spoke to a customer service representative ("CSR") on January 21, 2025.

42. The Progressive CSR informed Plaintiff that Progressive obtained Plaintiff's Driving Data from Tracking Technology installed in Plaintiff's Toyota vehicle.

43. Upon discovering that Defendant Toyota had been tracking Plaintiff's Driving Data *via* Tracking Technology installed in his Toyota vehicle, Plaintiff called Toyota on or about January 21, 2025 and spoke with a Toyota CSR to inquire why Toyota was sharing Plaintiff's Driving Data with third parties without his permission.

44. The Toyota CSR informed Plaintiff that when he purchased his Toyota vehicle, he unknowingly signed up for a trial of sharing his Driving Data captured by the Tracking Technology installed in Plaintiff's Toyota vehicle and that Plaintiff had to opt out of the data sharing.

45. Toyota, however, never provided Plaintiff with any sort of notice that Toyota would share his Driving Data with third parties.

46. The Toyota CSR also advised Plaintiff to check his Toyota mobile phone application to verify whether he was indeed participating in Toyota's telemetry data sharing

scheme.

47. Upon checking the Toyota application on his mobile phone, Plaintiff had been opted out of Toyota's data sharing scheme, contrary to the Toyota CSR's representation that Plaintiff signed up for the data sharing scheme.

48. Accordingly, in violation of state and federal law and of its own Data Sharing Policies, Toyota had been sharing Plaintiff's Driving Data with third parties without his consent.

49. On or about March 31, 2025, Plaintiff called Progressive over the phone to inquire about the exact data flow of his Driving Data. A Progressive CSR told Plaintiff that Progressive obtains Driving Data of drivers from Defendant CAS.

50. Despite CAS's "unwavering commitment" to customer privacy and representation that it does not share Driving Data without explicit vehicle owner consent,[22] it does so, nonetheless, because it shared Plaintiff's Driving Data illegally shared by Toyota. Plaintiff never provided consent to Defendants Toyota nor CAS to share the Driving Data collected from his Toyota vehicle with third parties.

51. Upon information and belief, Plaintiff's and Class Members' Driving Data was collected by Toyota *via* Tracking Technology installed in subject Toyota vehicles. Then, Toyota sold this Driving Data to Defendant CAS. Subsequently, Defendant CAS sold the Driving Data to Defendant Progressive.

Plaintiff and Class Members Suffered Harm as a Result of Defendants' Misconduct

52. Plaintiff and Class Members are current and former owners and lessees of vehicles manufactured by Toyota, with Tracking Technology installed in those vehicles.

[22] *Id*. ("Data is never shared without explicit vehicle owner consent.")

53. Unbeknownst to Plaintiff and Class Members, Defendant Toyota was collecting vast amounts of information including their location, speed and driving habits – even minute details such as acceleration, deceleration and "cornering" events – as well as images and sounds captured by their vehicles, and sharing it for profit to third parties, including Defendants CAS and Progressive.

54. Defendants' data collection and sharing practices described above constitute unlawful collection and dissemination of Plaintiff's and Class Members' Driving Data, including but not limited to: their vehicles' location, speed, direction, acceleration and braking, swerving/cornering events, images and voice data.

55. Plaintiff and Class Members suffered actual injury from having their Driving Data collected from their vehicles and sold to third parties including, but not limited to, (a) damage to and diminution in the value of their Driving Data—a form of property that Defendants obtained from Plaintiff; (b) violation of their privacy rights; (c) the likelihood of future theft of their Driving Data from these third parties.

56. In addition, Plaintiff and Class Members overpaid for their vehicles as a result of not knowing that these vehicles would collect and transmit highly intimate details of their movements, and that Defendant Toyota would share them with third parties without Class Members' consent.

57. Upon information and belief, Defendants continue to collect, hold and sell for profit this Driving Data, depriving Plaintiff and Class Members of informational autonomy, invading their privacy and appropriating the economic value of this information.

CLASS ACTION ALLEGATIONS

58. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

59. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All individuals in the United States who owned or leased model year 2018 or newer Toyota vehicles equipped with Tracking Technology.

60. The Class defined above is readily ascertainable from public records and from information in Defendants' possession. Thus, such identification of Class Members will be reliable and administratively feasible.

61. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendants or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

62. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

63. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

64. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on

information and belief, the Class consists of hundreds of thousands of individuals who reside in the U.S. and purchased Toyota vehicles equipped with Tracking Technology.

65. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendants unlawfully collected and disseminated Plaintiff's and Class Members' PII contrary to the Federal Wiretap Act;

b. If Defendants unlawfully collected and disseminated Plaintiff's and Class Members' PII contrary to the Computer Fraud and Abuse Act;

c. If Defendants' collection and dissemination of Plaintiffs' PII was an invasion of privacy under Texas common law;

d. If Plaintiff and Class Members did not obtain the benefit of their bargain when they purchased their vehicles without Defendants disclosing to them that they were collecting and disseminating their PII;

e. If Plaintiff and Class Members were injured as a proximate cause or result of Defendants' misconduct described in this Complaint; and

f. If Plaintiff and Class Members are entitled to compensatory damages, treble damages, reimbursement of out-of-pocket costs and/or injunctive relief.

66. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was collected in the same way, through data tracking technology, and disseminated in the same way by the Defendants to insurance companies and others. Moreover, Plaintiff and all Class Members were subjected to Defendants' uniformly illegal and impermissible conduct.

67. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's Counsel are competent and experienced in litigating complex data privacy class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

68. **Predominance**. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was collected in the same way from Toyota vehicles and unlawfully and inadequately shared, using data tracking technology, with insurance companies, such as Defendant Progressive. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

69. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

70. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

71. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

72. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above, including in paragraph 46.

73. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Violations of the Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq*.
(On Behalf of Plaintiff and the Class Against All Defendants)

74. Plaintiff re-alleges and incorporates by reference paragraphs 1-73 of the Complaint as if fully set forth herein.

75. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

76. In relevant part, the FWA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

77. The FWA also makes it unlawful for any person to intentionally disclose, or endeavor to disclose, to any other person or to intentionally use, or endeavor to use, the "contents

of any wire, oral, or electronic communication, knowing or having reason to know that" the communication was obtained in violation of the FWA. 18 U.S.C. § 2511(1)(c) & (d).

78. The FWA provides a private right of action to any person whose wire, oral, or electronic communication is intercepted, used, or disclosed. 18 U.S.C. § 2520(a).

79. The FWA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

80. The FWA defines "electronic communication" as "any transfer of signs, signals, […] data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

81. The FWA defines "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

82. The FWA defines "contents," with respect to any covered communication, to include "any information concerning the substance, purport, or meaning of that communication[.]" 18 U.S.C. § 2510(8).

83. The FWA defines "person" to include "any individual, partnership, association, joint stock company, trust, or corporation[.]" 18 U.S.C. § 2510(6).

84. Defendants are persons as defined in 18 U.S.C. §2510(6).

85. The data and transmissions within, to, and from Plaintiff's and Class Members' vehicles constitute "electronic communications," as defined by 18 U.S.C. § 2510(12), as they are

transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photooptical systems that affect interstate commerce.

86. As alleged herein, Defendants intercepted, in real time and as it was transmitted, the contents of electronic communications transmitted within, to, and from Plaintiffs' vehicles, and diverted those communications to themselves without consent. In particular Toyota intercepted Defendant's Driving Data, while CAS and Progressive procured Toyota to intercept it. Each Defendant intentionally used the Driving Data, knowing it was obtained without driver consent.

87. As detailed herein, the electronic communications detailed above that Defendants have intercepted are tied to individual drivers and vehicles, and not anonymized.

88. Plaintiffs and Class Members have a reasonable expectation of privacy within their vehicles, and Plaintiffs and Class Members reasonably expected privacy while driving their vehicles.

89. Common understanding and experience of how mobile apps work create a reasonable expectation that an auto manufacturer and its affiliates and business partners, such as Defendants, would not surreptitiously intercept and divert the detailed and personal electronic communications described above.

90. In further violation of the FWA, Defendants have intentionally used or endeavored to use the contents of the electronic communications described above knowing or having reason to know that the information was obtained through interception in violation of 18 U.S.C. § 2511(1)(a). 18 U.S.C. § 2511(1)(d).

91. Specifically, Defendants used the illegally obtained information to profit and price insurance products sold to Plaintiff and Class Members, and sold this information to other third parties.

92. As a result, Plaintiff and Class Members have suffered harm and injury due to the interception, disclosure, and/or use of electronic communications containing their private and personal information.

93. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members have been damaged by Defendants' interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made by Defendants as a result of the violation or (b) statutory damages for each Class Member of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

SECOND CAUSE OF ACTION
Violation of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030, *et seq*.
(On Behalf of Plaintiff and the Class against Defendant Toyota)

94. Plaintiff re-alleges and incorporates by reference paragraphs 1-73 of the Complaint as if fully set forth herein.

95. The Computer Fraud and Abuse Act ("CFAA") prohibits the intentional accessing, without authorization or in excess of authorization, of a computer under certain circumstances. 18 U.S.C. § 1030(a).

96. The CFAA specifically provides that it is unlawful to "intentionally access a computer without authorization or exceed[] authorized access, and thereby obtain[]…information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

97. Plaintiff, as an individual, and Defendant Toyota, as a corporations, are "persons" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(12).

98. A "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(10).

99. Plaintiff's and Class Members' Toyota vehicles are data-processing devices performing logical, arithmetic, and storage functions and thus constitute a "computer" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(1).

100. "Exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain." 18 U.S.C. § 1030(e)(6).

101. A "protected computer" is defined as "a computer . . . which is used in or affecting interstate or foreign commerce or communication…, [or that] has moved in or otherwise affects interstate or foreign commerce." 18 U.S.C. § 1030(e)(2)(B).

102. Plaintiff's and Class Members' vehicles are used to send and receive information and electronic communications across state lines and internationally. Thus, they constitute "protected computers" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(2)(B).

103. Through Toyota's Tracking Technology, Defendant Toyota intentionally accessed the Plaintiff's and Class Members' vehicles without Plaintiffs' or Class Members' authorization, or in a manner that exceeded Plaintiff's and Class Members' authorization, and obtained information therefrom in violation of the CFAA. 18 U.S.C. § 1030(a)(2)(C).

104. Plaintiff and Class Members have suffered harm and injury due to Defendant Toyota's unauthorized access to the communications containing their private and personal information in the form of Driving Data, as well as Toyota's sale of such information to other insurers.

105. A civil action for violation of the CFAA is proper if the conduct involves "loss to 1 or more persons during any 1-year period … aggregating at least $5,000 in value." Because the loss to Plaintiff and Class Members during any one year period within the relevant timeframe, including the loss of their privacy interest in and control over their Driving Data, exceeded $5,000 in aggregate, Plaintiff and the Class are entitled to bring this civil action and are entitled to economic damages, compensatory damages, injunctive, equitable, and all available statutory relief, as well as their reasonable attorney's fees and costs and other relief as permitted by the CFAA. 18 U.S.C. § 1030(g).

THIRD CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Plaintiff and the Class Against All Defendants)

106. Plaintiff re-alleges and incorporates by reference paragraphs 1-73 of the Complaint as if fully set forth herein.

107. Plaintiff and Class Members have a common law, legally and constitutionally protected privacy interest in their Driving Data and are entitled to the protection of their Driving Data against unauthorized access.

108. Plaintiff and Class Members have a reasonable expectation of privacy in their driving abilities, habits, patterns, and behavior engaged in while they are in their own vehicles, and in any compilation of highly personalized driving behavior profile resulting from the collection of such data.

109. As Plaintiff and Class Members drive to work, visit family, or simply go about their days, while Defendants are tracking Plaintiffs and Class Members, Plaintiff and Class Members have unknowingly created troves of highly sensitive data mapping their respective personal lives which is then collected, captured, transmitted, accessed, compiled, stored, analyzed, and sold—all without their knowledge or informed consent.

110. The continued nonconsensual surveillance of an individual in their private capacity, as Defendants have done and continue to do, represents a fundamental violation of personal privacy, freedom, and autonomy.

111. As a result of Defendants' intentionally intrusive conduct, Plaintiff and Class Members have been and still remain today under pervasive surveillance compromising their privacy, autonomy, and basic human dignity.

112. Defendants intentionally invaded Plaintiff's and Class Members' privacy interests by deliberately and surreptitiously obtaining, improperly gaining knowledge of, reviewing, retaining, packaging, and selling their confidential Driving Data.

113. Defendants' conduct is highly offensive to a reasonable person and constitutes an egregious breach of social norms underlying the right to privacy, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

114. By tracking, collecting, and storing Plaintiff's and Class Members' Driving Data without authorization or consent to do so, Defendants intentionally intruded upon Plaintiff's and Class Members' seclusion, solitude, and private life engaged in within the confines of their respective vehicles, without their knowledge or permission.

115. Defendants have improperly profited from their invasion of Plaintiff's and Class Members' privacy and their use of Plaintiff's and Class Members' Driving Data for their economic value and their own commercial gain, including by selling Driving Data to other third parties.

116. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class Members' reasonable expectations of privacy were frustrated, exploited, compromised, and defeated.

117. Plaintiff and Class Members were harmed by Defendants' wrongful conduct causing their loss of privacy and the confidentiality of their own private conduct within the confines of their own vehicle. Defendants have needlessly harmed Plaintiff and Class Members by capturing their Driving Data through their connected services. This intrusion, disclosure of information, and loss of privacy and confidentiality has caused Plaintiff and Class Members to suffer mental anguish, actual damages, loss of value of their personal data, and an invasion of their privacy in an amount to be determined at trial.

118. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will cause irreparable injury to Plaintiff and Class Members in that their Driving Data maintained by Defendants may be viewed, distributed, and used by unauthorized third parties for years to come.

119. Plaintiff and Class Members seek nominal, compensatory, and punitive damages as a result of Defendants' actions. Plaintiff and Class Members seek actual damages suffered, plus any profits attributable to Defendants' use of Plaintiff's and Class Members' Driving Data. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were done in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

FOURTH CAUSE OF ACTION
Breach of Express and Implied Contract
(On Behalf of the Plaintiff and the Class against Defendant Toyota)

120. Plaintiff re-alleges and incorporates by reference paragraphs 1-73 of the Complaint as if fully set forth herein.

121. Plaintiff and Class Members entered into express and implied contracts with Toyota for the purchase and/or leasing of Toyota vehicles equipped with Tracking Technology, which tracked Plaintiff's and Class Members' Driving Data, including: location, speed, direction, braking and swerving/cornering events, and image and voice data.

122. As part of these transactions, Toyota explicitly and implicitly agreed to obtain Plaintiff's and Class Members' express prior consent before sharing Plaintiff's and Class Members' Driving Data with third parties, as follows:

> We share Driving Data with our affiliates and business partners so we can work together to provide Connected Services to you and for product improvement. ***If you provide express prior consent, we may also share your Driving Data with our affiliates and non-affiliated insurance companies to provide you with usage-based insurance information and offers***. We will also share Driving Data with compatible third-party services and device[s] [that] you authorize. ***Unless we obtain your consent, we will not provide your Driving Data to other parties for their own purposes or use your Driving Data for our marketing purposes***.

123. Plaintiff and Class Members entered into express and implied contracts with the reasonable expectations (based on Toyota's own express and implied promises) that Toyota would not share with third parties Plaintiff's and Class Members' Driving Data unless Toyota first obtained Plaintiff's and Class Members' express prior consent to do so.

124. Plaintiff and Class Members would not have paid such high prices for their vehicles nor would they have purchased or leased the vehicles if Plaintiff and Class Members had been informed of Toyota's intentions to violate the express and implied contracts by collecting and

transmitting their Driving Data and sharing this data with third parties without Plaintiff's and Class Members' express prior consent.

125. As detailed above, Toyota breached its express and implied contracts with Plaintiff and Class Members to share their Driving Data with third parties only upon obtaining Plaintiff's and Class Members express prior consent to do so when Toyota shared Plaintiff's and Class Members' Driving Data to Defendants CAS and Progressive without Plaintiff's and Class Members' express prior consent.

126. Indeed, Plaintiff had not given Toyota his express prior consent to have his Driving Data shared with third parties because Plaintiff had been (and remains) opted out of Toyota's third-party data sharing scheme.

127. As a direct result of Toyota's breach of express and implied contracts, Plaintiff and Class Members sustained actual losses and damages as described herein.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Plaintiff and the Class Against Defendant Toyota)

128. Plaintiff pleads this cause of action in the alternative to the Fourth Cause of Action, above.

129. Plaintiff re-alleges and incorporates by reference paragraphs 1-73 of the Complaint as if fully set forth herein.

130. Plaintiff and Class Members conferred a direct benefit on Defendant Toyota by paying Toyota sums of money, in purchase or lease transactions, in exchange for Toyota vehicles equipped with Tracking Technology, which collected extensive personal Driving Data, including, but not limited to, locations, speeds, and other driving behaviors, without the informed consent of Plaintiff and Class Members.

131. Toyota has unjustly enriched itself by having Plaintiffs and Class Members overpay for their Toyota vehicles as a result of not knowing that these vehicles would collect and transmit highly intimate details of their movements, and that Defendant Toyota would share them with third parties without Class Members' consent.

132. Further, Defendant Toyota's appropriation of Plaintiff's and Class Members' Driving Data, which it then monetized by reselling, constitutes the direct conferral of a benefit without just compensation.

133. Toyota, without the consent or knowledge of Plaintiff and Class Members, sold Plaintiff's and Class Members' highly personal and proprietary driving data to third parties, including Defendants CAS and Progressive.

134. Thus, Toyota has unjustly enriched itself by commercially exploiting Plaintiff's and Class Members' proprietary Driving Data, directly at the expense of their privacy and financial interests.

135. If Plaintiff and Class Members had been informed of Toyota's intentions to collect and transmit their Driving Data and share this data with third parties without Plaintiff's and Class Members' consent, Plaintiff and Class Members would not have paid such high prices for their vehicles nor would they have purchased the vehicles at all.

136. Plaintiff and Class Members did not freely or knowingly allow Toyota to exploit their personal and proprietary Driving Data for commercial gain. If Plaintiff and Class Members had been informed of Toyota's intentions to profit from their personal driving data, they would not have consented to such use.

137. Plaintiff and Class Members overpaid for their Toyota vehicles. If Plaintiff and Class Members had been informed that Toyota would track their Driving Data obtained from

Plaintiff's and Class Members' use of their Toyota vehicles equipped with Tracking Technology, they would not have purchased the vehicles.

138. The enrichment of Defendant Toyota at the expense of Plaintiff and Class Members is against equity and good conscience. Toyota's retention of the benefit without proper compensation to Plaintiff and Class Members is unjust and warrants restitution.

139. As a direct and proximate result of Toyota's unjust enrichment, Plaintiff and Class Members have suffered damages – they have overpaid for their vehicles and have been deprived of the economic value of their personal and proprietary Driving Data.

140. Defendant Toyota should be compelled to disgorge, in a common fund for the benefit of Plaintiff and Class Members, all unlawful or inequitable proceeds that Toyota received as a result of the misconduct described herein.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative, and the undersigned as Class Counsel;

B. An order enjoining Defendants from: (i) continuing to collect Plaintiff's and Class Members location and vehicle data (including: location, speed, direction, braking and swerving/cornering events, and image and voice data), and other PII, recorded by their vehicles, (ii) storing it or (iii) offering it for sale to third parties; and

C. A mandatory injunction requiring that Defendants to delete all location and vehicle data (including: location, speed, direction, braking and swerving/cornering events, and image and voice data) and other PII unlawfully collected from Plaintiffs and Class Members;

D. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

E. An award of pre- and post-judgment interest, attorneys' fees, costs, expenses, and interest as permitted by law;

F. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

G. For all other Orders, findings, and determinations identified and sought in this Complaint; and

H. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: April 21, 2025

Respectfully Submitted,

/s/ Bruce W. Steckler
Bruce W. Steckler
Texas Bar No. 00785039
Bruce@stecklerlaw.com
Austin P. Smith
Texas Bar No. 24102506
austin@stecklerlaw.com
Paul D. Stickney
Texas Bar No. 00789924
judgestickney@stecklerlaw.com
Jack M. Kelley
Texas Bar No. 24137613
jkelley@stecklerlaw.com
STECKLER WAYNE & LOVE PLLC
12720 Hillcrest Road, Suite 1045
Dallas, Texas 75230
T: 972-387-4040
F: 972-387-4041

John A. Yanchunis*
Texas Bar No. 22121300
JYanchunis@forthepeople.com
Ronald Podolny*
ronald.podolny@forthepeople.com
Antonio Arzola, Jr.*
ararzola@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
T: (813) 223-5505
F: (813) 223-5402

**Pro hac vice forthcoming*
Counsel for Plaintiff and the Class